

EXHIBIT N

18 MAG 7548

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of Warrant for All Content and Other
Information Associated with the Email Account
[REDACTED], Maintained at Premises
Controlled by Apple, Inc., USAO Reference No.
2016R00246.

TO BE FILED UNDER SEAL

AGENT AFFIDAVIT

**Agent Affidavit in Support of Application for Search Warrants
for Stored Electronic Communications**

STATE OF NEW YORK)
) ss.
COUNTY OF NEW YORK)

DIANA CHAU, Postal Inspector, United States Postal Inspection Service, being duly
sworn, deposes and states:

I. Introduction

A. Affiant

1. I am a Postal Inspector with the U.S. Postal Inspection Service (the “USPIS” or “Investigating Agency”). As such, I am a “federal law enforcement officer” within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. During my tenure with the USPIS, I have participated in the investigations of numerous frauds, and have conducted physical and electronic surveillance, the execution of search warrants, debriefings of informants, and reviews of taped conversations. Through my training, education, and experience, I have become familiar with the manner in which securities frauds are perpetrated.

B. The Provider, the Subject Account, and the Subject Offenses

2. I make this affidavit in support of an application for a search warrant pursuant to 18 U.S.C. § 2703 for all content and other information associated with the email account associated with email address [REDACTED] (the “Subject Account”), maintained and controlled by Apple, Inc. (“Apple” or the “Provider”), headquartered in Cupertino, California.. The Subject Account is believed to be used by [REDACTED]. The information to be searched is described in the following paragraphs and in Attachment A to the proposed warrant.

3. As detailed below, there is probable cause to believe that the Subject Account contains evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1343 (wire fraud), 1348 (securities fraud), 1350 (improper certification of financial reports by corporate officers); and Title 15, United States Code, Sections 78j(b) and 78ff and Title 17, Code of Federal Regulations, 240.10b-5 (securities fraud), and aiding and abetting and conspiring to commit these offenses in violation of Title 18, United States Code, Section 2 (aiding and abetting), 371 (conspiracy) and 1349 (conspiracy) (together, the “Subject Offenses”).

4. This affidavit is based upon my personal knowledge, my review of documents and other evidence, and my conversations with other law enforcement officers, as well as my training and experience concerning the use of email in criminal activity. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts I have learned during my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

C. Services and Records of the Provider

5. I have learned the following about the Provider:

a. The Provider offers email services to the public. In particular, the Provider allows subscribers to maintain email accounts under different domain names including “me.com.” A subscriber using the Provider’s services can access his or her email account from any computer connected to the Internet.

b. Apple maintains the following records and information with respect to subscriber accounts:

i. *Email contents.* In general, any email (which can include attachments such as documents, images, and videos) sent to or from a subscriber’s account, or stored in draft form in the account, is maintained on the Provider’s servers unless and until the subscriber deletes the email. If the subscriber does not delete the email, it can remain on the Provider’s computers indefinitely. Even if the subscriber deletes the email, it may continue to be available on the Provider’s servers for a certain period of time.

ii. *Address book.* The Provider also allows subscribers to maintain the equivalent of an address book, comprising email addresses and other contact information of other email users.

iii. *Subscriber and billing information.* The Provider collects and maintain (typically unverified) identifying information about each subscriber, including, for example, name, username, address, telephone number, and alternate email addresses. The Provider also maintains records concerning the date on which the account was created, the Internet protocol (“IP”) address of the user at the time of account creation, the current status of the account (*e.g.*, active or closed), the length of service, and the types of services utilized by the subscriber. Additionally, for paying

subscribers, the Provider maintains records of the subscriber's means and source of payment, including any credit card or bank account number.

iv. *Transactional information.* The Provider also typically retains certain transactional information about the use of each account on its system. This information can include records of login (*i.e.*, session) times and durations and the methods used to connect to the account (such as logging into the account through the Provider's website).

v. *Customer correspondence.* The Provider also typically maintains records of any customer service contacts with or about the subscriber, including any inquiries or complaints concerning the subscriber's account.

vi. *Web History.* Apple also maintains searches and account browsing activity, from Safari, Apple's proprietary web browser, as well as other applications.

vii. *iOS Backup Services.* Apple also maintains, in certain instances, backups of iOS devices (such as iPhones and iPads) associated with its email accounts. Such backups often contain emails stored on the user's physical devices (even if no longer stored in the user's online mailbox), as well a user's iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, browser history, contacts, calendar events, reminders, notes, app data and settings, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud.

viii. *Preserved and backup records.* The Provider also maintains preserved copies of the foregoing categories of records with respect to an account, for at least 90 days, upon receiving a preservation request from the Government pursuant to 18 U.S.C. § 2703(f). The

Provider may also maintain backup copies of the foregoing categories of records pursuant to its own data retention policy.

D. Jurisdiction and Authority to Issue Warrants

6. Pursuant to 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A), the Government may require a provider of an electronic communications service or a remote computing service, such as the Provider, to disclose all stored content and all non-content records or other information pertaining to a subscriber, by obtaining a warrant issued using the procedures described in the Federal Rules of Criminal Procedure.

7. A search warrant under § 2703 may be issued by “any district court of the United States (including a magistrate judge of such a court)” that “has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

8. When the Government obtains records under § 2703 pursuant to a search warrant, the Government is not required to notify the subscriber of the existence of the warrant. 18 U.S.C. § 2703(a), (b)(1)(A), (c)(2) & (3). Additionally, the Government may obtain an order precluding the Provider from notifying the subscriber or any other person of the warrant, for such period as the Court deems appropriate, where there is reason to believe that such notification will seriously jeopardize an investigation. 18 U.S.C. § 2705(b).

II. Probable Cause

9. I respectfully submit that probable cause exists to believe that the requested information will lead to evidence of violations of the Subject Offenses relating to accounting and financial reporting fraud at MiMedx Group, Inc. (“MiMedx”), a publicly traded biopharmaceutical company.

Overview of the Accounting Fraud Scheme

10. As described in greater detail below, there is probable cause to believe that from at least 2012 through 2017, MiMedx, through its senior management and directors, routinely and knowingly filed public financial reports with the United States Securities and Exchange Commission (the “SEC”) that contained false and inflated earnings information, with the intent to deceive the investing public. Specifically, during the relevant period, MiMedx improperly recognized revenue from the purported sale of its products in violation of generally accepted accounting principles (“GAAP”) and relevant regulations and guidance promulgated by the SEC. MiMedx then falsely reported this inflated revenue to the investing public, including through its financial filings with the SEC.

Relevant Entities and Persons

11. Based on my review of publicly available information, my review of records produced by MiMedx in response to a subpoena by the SEC, and my conversations with representatives of MiMedx, I have learned the following, in substance and in part:

a. MiMedx Group, Inc. is a biopharmaceutical company that develops and markets regenerative and therapeutic biologics using human placental tissue allografts. At all relevant times, MiMedx was a publicly traded company, listed on the NASDAQ exchange. One product MiMedx sold during the relevant period was known as “Epifix,” a skin substitute product.

b. On or about February 20, 2018, MiMedx issued a press release and filed a Form 8K with the SEC, announcing that the filing of the company’s reports of financial results for fourth quarter 2017 and fiscal year 2017 would be delayed and that the company’s audit committee had begun “an internal investigation into current and prior-period matters relating to allegations

regarding certain sales and distribution practices at the Company.” To date, MiMedx has not filed its financial results for fourth quarter 2017 or fiscal year 2017.

c. On or about June 6, 2018, MiMedx announced that its previously issued financial statements for the years 2012 through 2016 and for the first three quarters of 2017 needed to be restated and should no longer be relied upon. Pursuant to applicable federal law, [REDACTED], [REDACTED], had certified each of MiMedx’s quarterly SEC filings during that period (i.e., Form 10Q), and, [REDACTED] and PARKER “PETE” PETIT, MiMedx’s Chief Executive Officer, had certified each of MiMedx’s annual SEC filings (i.e., Form 10K) during that period. In announcing the need to restate those filings, MiMedx explained that “the determination of the need to restate was based on investigation results to date which have primarily been focused on the accounting treatment afforded to such sales and distribution practices for *two distributors* for which certain implicit arrangements modified the explicit terms of the contracts, impacting revenue recognition during specified periods.” (emphasis added). Since the beginning of June 2018, PETIT, [REDACTED] MiMedx’s Chief Operating Officer (WILLIAM TAYLOR), and MiMedx’s Controller ([REDACTED]), have all left the employment of the company.

d. AvKare, Inc, is a Tennessee-based medical supply company, which, based on conversations with representatives of MiMedx’s audit committee, I understand was one of the two distributors referenced in MiMedx’s June 6, 2018 announcement. In or about April 2012, MiMedx and AvKare entered into a purported Product Distribution Agreement, under which, in sum and substance, AvKare became the exclusive distributor for MiMedx’s Epifix product in the Veterans Affairs (“VA”) hospital system. AvKare, unlike MiMedx at the time, was on the Federal Supply Schedule, which allowed it to sell products into the VA system. As discussed below and in

practice, however, MiMedx sales representatives (“account executives”), and not AvKare employees, were the individuals who distributed Epifix and other MiMedx products in the VA system.

e. During the relevant period, [REDACTED] worked as a Vice President in MiMedx’s Sales Department. As a Vice President in the Sales Department, [REDACTED] oversaw approximately five to six Regional Sales Directors, who, in turn, oversaw MiMedx’s account executives for particular regions.

f. [REDACTED] was a Regional Sales Director who reported to DION at certain times during the relevant period.

g. [REDACTED] was MiMedx’s [REDACTED] from in or about mid-2015 to February 2016. As discussed below, in or about February 2016, [REDACTED] separated from MiMedx and his position was filled by [REDACTED].

h. At all relevant times, [REDACTED] and [REDACTED] were members of MiMedx’s Board of Directors and members of the Board’s audit committee. According to published reports, [REDACTED] is a former fraternity brother and longtime friend of PETIT.

Relevant Accounting Principles

12. Generally accepted accounting principles (GAAP) refer to a common set of accounting principles, standards and procedures that companies must follow (represent that they follow) when preparing and filing financial statements. GAAP is meant to ensure a minimum level of methodological consistency across the financial statements of different companies, which makes it easier for investors to analyze and extract useful information and compare GAAP metrics across

different companies. For publicly traded companies, the SEC also promulgates accounting rules and guidance that companies must follow when filing their financial reports.

13. Under GAAP and SEC guidance, a company that engages in the sale of products through a distributor may recognize revenue upon transfer of the product to a distributor if, among other things, collectability (i.e., receiving payment) is reasonably assured. When the distributor has a right of return (i.e., the ability to return the product without having to pay for it), revenue cannot be properly recognized unless all of the following criteria are met: (1) the seller's price to the buyer is fixed or determinable at the date of sale; (2) the buyer's obligation to pay the seller is not contingent on the resale of the product; (3) the buyer's obligation to pay the seller is not excused in the event that the product is damaged or lost; (4) the buyer has economic substance separate from the seller; (5) the seller does not have significant obligations for future performance to directly bring about the resale of the product by the buyer; and (6) the amount of future returns can be reasonably estimated. *See, e.g.*, Accounting Standards Codification, Subtopic 605-15-25-1.

MiMedx's Relationship with AvKare and Inappropriate Revenue Recognition

14. Based upon interviews with MiMedx personnel, review of company documents, and conversations with representatives of MiMedx, investigators have learned the following facts about MiMedx's relationship with AvKare during the period from 2012 to 2017:

a. As discussed, during the relevant period, distribution through AvKare was the primary means by which MiMedx sold its products to VA hospitals. These sales, in turn, accounted for a significant part of MiMedx's revenue.

b. Although AvKare nominally acted as a distributor of MiMedx's products within the VA system, in practice, AvKare employees played little role in marketing or distributing

MiMedx products. Rather, MiMedx maintained what the company called a “federal sales force,” whose members were responsible for interacting with VA employees, monitoring the stock of MiMedx product on the shelves at VA hospitals, and keeping track of when tissue was implanted in patients.

c. When MiMedx’s personnel determined that a particular VA facility was in need of tissue, they notified MiMedx’s sales department, which then shipped the product directly to the VA facility. Although AvKare was notified of the shipment, no AvKare employees were physically involved in handling the product. During the relevant period, MiMedx treated such shipments as sales to AvKare and recognized revenue at the time of shipment. In practice, however, AvKare was under no obligation to pay MiMedx for the tissue until the VA purchased it from AvKare, generally at the time of implantation. Moreover, because AvKare did not have a sales force of its own, MiMedx employees were exclusively responsible for promoting MiMedx products to VA doctors and facilities.

d. Moreover, despite the fact that MiMedx recognized revenue for tissue at the time of shipment to the VA, during the relevant period, MiMedx routinely issued AvKare credits for lost or damaged tissue, even after it had been shipped to the VA. As TAYLOR explained to an AvKare principal in an email dated March 8, 2013:

Contractually, AvKare owns the inventory once received (under the new agreement, once shipped), but practically speaking, MiMedx will work with AvKare if any issues arise with the inventory. Some recent examples highlight this. Over the past few months, several grafts have been dropped or otherwise lost and MiMedx replaced them at no cost to AvKare. Because MiMedx is directing the placements in the 120+ VAs we service, we obviously are very involved with the inventory management and will not leave you with any losses!

e. Nor was it the case that AvKare’s obligation to pay MiMedx for shipped tissue existed independent of AvKare’s ability to resell the product to the VA. Indeed, beginning in April

2015, the product distribution agreement between AvKare and MiMedx explicitly provided that in the event the relationship were to terminate, MiMedx would “repurchase any remaining inventory of Products from AvKare at the price paid by AvKare for such Product.”

f. From conversations with representatives of MiMedx, investigators have learned that the company’s decision to re-state its earnings was prompted, in part, by the conclusion that, based on the information above, MiMedx’s practice of recognizing revenue at the time tissue was shipped to AvKare was inconsistent with GAAP and SEC guidance.

Evidence of “Channel Stuffing” and Inappropriate Revenue Recognition

15. In addition to the conduct set forth above, there is further probable cause to believe that MiMedx also carried out a practice known as “channel stuffing” in order to fraudulently inflate its reported revenue. Generally speaking, channel stuffing occurs when a company sends more products to its customer than the customers are able to sell to the public, in order to fraudulently inflate the company’s sales and earnings figures. Often, channel stuffing occurs just before quarter-end or year-end so that the company can “make” or “hit” particular earnings or revenue targets or meet Wall Street analyst projections relating to those metrics.

16. MiMedx’s practice of recognizing revenue at the time that tissue was shipped to VA facilities, combined with the company’s role in controlling the supply of tissue to those facilities, effectively permitted MiMedx artificially to engineer revenue figures in order to meet market expectations. The following examples illustrate this point:

17. In or about June 2018, another Postal Inspector (“Inspector-1”) interviewed an individual who worked at MiMedx as an account executive between 2012 and 2016 (“Witness-

1”).¹ Based on my review of Inspector-1’s memorandum of that interview and my conversations with Inspector-1, I have learned the following:

a. Witness-1’s primary role during the relevant period was to sell MiMedx products to VA hospitals in the mid-Atlantic region, including products purportedly distributed through AvKare. During the relevant period, Witness-1 reported to [REDACTED] and [REDACTED].

b. On repeated occasions, [REDACTED] and [REDACTED] requested that Witness-1 have MiMedx products shipped to the VA near the end of quarters, even though the VA had not ordered or requested such products from Witness-1. During these conversations, it was conveyed to Witness-1, in substance, that MiMedx “needed to hit a number,” i.e, a quarterly revenue target. Witness-1 never contacted anyone at the VA about these orders, and, if he was present at the VA when these products arrived, he would hide some of the products that the VA did not need in a VA closet so that VA personnel would not know it was there. Because, during the relevant period, MiMedx generally recognized revenue when a product was shipped from MiMedx, I believe practices like the one described by Witness-1 may have had the effect of fraudulently inflating MiMedx’s revenue.

18. I have also reviewed a December 30, 2015 audio recording made by [REDACTED] [REDACTED],² who at the time was a MiMedx Regional Sales Director. The recording is of a

¹ Witness-1 was fired by MiMedx on or about December 29, 2016 for purportedly, I understand, for violating “non-compete” provisions of his employment contract with MiMedx. I also understand that Witness-1 is engaged in additional civil litigation against MiMedx. Witness-1’s information has been corroborated by other information provided to the Government, including the electronic messages referenced herein.

² I understand that [REDACTED] was also terminated by MiMedx in December 2016 for purportedly violating the terms of his non-compete agreement with MiMedx. [REDACTED] has filed a wrongful retaliation lawsuit against MiMedx, which was recently dismissed due to a forum-selection clause in [REDACTED] employment agreement. The above recording was made approximately a year before [REDACTED] termination.

call between [REDACTED] and [REDACTED]. In the call, [REDACTED] tells [REDACTED] that he is “dialing for dollars[,] looking for money” and asked [REDACTED] about “what additional could you put on to help us hit the number for the quarter because we’re short overall. And so do you have additional space . . . to do more if you had to?” [REDACTED] went onto say that “Pete says . . . ‘[t]his is a company directive. So, if they don’t and orders come through between now and [unintelligible]’—this is the only time I’ve ever heard him cuss. He said: Their ass is grass.’ So I’m just — I’m just putting it out there.” Later in the call [REDACTED] stated, “By—by June—by June, we’re gonna take credit for all this stuff back anyways. We’re bring all this back. It’s—we’re gonna credit AvKare.”

19. Based on my training and experience, I believe that, during this call, [REDACTED] is telling [REDACTED] that MiMedx was not expected to make its revenue forecasts for fourth quarter 2016 (“help us hit the number for the quarter because we’re short overall”). [REDACTED] goes on to suggest that [REDACTED] place additional MiMedx products with the VA to help MiMedx meet those revenue forecasts, even if the VA had not yet ordered those products (“do you have additional space”). [REDACTED] adds that MiMedx’s CEO, Parker “Pete” Petit (“Pete”) has said that, if any MiMedx sales person refused to comply with this “company directive,” “their ass is grass.” Further, to attempt to assuage [REDACTED] concerns, [REDACTED] states that the sales will be reversed by June (“by June, we’re gonna take credit for all this stuff back anyways”), further indicating MiMedx was attempting to book revenue for sales that were not actually occurring.

20. Based on MiMedx’s public filings, I have learned that on or about January 10, 2016, MiMedx announced that it had “recorded record revenue for the year ended December 31, 2015 of \$187.3 million, a \$69.1 million or 58% increase over 2014 revenue of \$118.2 million” and that

it had “recorded record revenue for the 2015 fourth quarter of \$51.8 million, a \$12.3 million or 31% increase over 2014 fourth quarter revenue of \$39.6 million.”

Probable Cause Regarding the Subject Account

21. I submit that there is probable cause to believe that that the Subject Account will contain evidence that senior management and/or board members of MiMedx knew or had reason to know that the company was improperly recognizing revenue with regard to AvKare since at least January 2016 and nevertheless persisted in that accounting treatment.

22. Specifically, on or about January 18, 2016, [REDACTED], who was at the time the [REDACTED], sent an email to [REDACTED] the company’s CFO with subject line “Revenue Recognition and Controls.” In the body of the email, [REDACTED] raised concern “about MiMedx’s revenue recognition and the \$187.3 million in revenue that we are reporting for full year 2015.” Specifically, [REDACTED] expressed the belief that the \$6.2 million in revenue that the company was attributing to AvKare in 2015 was inflated because AvKare “has a right of return and doesn’t meet all of the exception criteria, and implicitly doesn’t pay MiMedx until the tissue has been implanted.” [REDACTED] also raised concerns about several other distributors, including SLR (accounting for \$4.5 million in sales) and Stability Biologics (\$2.4 million). [REDACTED] also questioned the timing of revenue recognition for a sale of tissue to a company called First Medical in the second quarter of 2015, as well as sales to AvKare in prior years. The email also referenced “concerns” that [REDACTED] had “shared previously.”

23. On February 8, 2016, [REDACTED] using the Subject Account sent an email to [REDACTED] with subject line “Meeting,” cc’ing [REDACTED]. In the body of the email, [REDACTED] forwarded [REDACTED] original email to [REDACTED] and wrote:

Hello [REDACTED]

██████████ and I representing the Audit Committee would like to meet with you this week to discuss your email attached. It is my understanding that your attorney has indicated that 11 am on Thursday at the MiMedx offices would work. Will you please confirm this is acceptable. Thank you.

██████████
Sent from my iPad
██████████

24. A memorandum produced by MiMedx's external auditor indicates that on February 11, 2016, members of MiMedx's Audit Committee met with ██████████. According to the memorandum, during the meeting, ██████████ indicated that he did not believe anyone had acted in bad faith or with intent to deceive but that he would not sign the company's audit representation letter as Controller. According to the memorandum, MiMedx's external auditors addressed the issues raised by ██████████ and concluded "there was no impact on their audit conclusions." The Audit Committee also concluded that "██████████ recommended accounting methods would not be appropriate and would result in [MiMedx's] financial statements not being in accordance with GAAP." Also according to the memo, on February 11, 2016, the company and ██████████ concluded negotiations over a severance agreement and ██████████ ceased to work at MiMedx. At the time of his separation, ██████████ had worked at the company for less than a year.

25. As noted, following ██████████ complaints, MiMedx continued to recognize revenue improperly for all of 2016 and a portion of 2017, before publicly announcing that it would restate its earnings from 2012 onward.

26. As noted, the memorandum discussed above was produced by MiMedx's external auditor. To date, MiMedx has not produced documents that reflect what reaction ██████████ and other members of MiMedx's senior management had to ██████████ January 18, 2016 email, nor has the company produced any emails that reflect how the text of ██████████ made its way

from [REDACTED] to Subject Account-1 and what commentary, if any, accompanied the forwarding of [REDACTED] email.

27. Based on my training and experience, I know that email records oftentimes contain evidence of the crime of securities fraud, conspiring to commit securities fraud, and aiding and abetting securities fraud. In this case, [REDACTED] email to [REDACTED] and [REDACTED] email to [REDACTED] are evidence that senior leadership in the company were on notice that the company's accounting practices were questionable as early as January 2016, more than a year before the company publicly acknowledged errors in its revenue recognition practices. Although the memorandum documenting the Audit Committee's investigation into [REDACTED] concerns appears to conclude that the company's accounting treatment was proper, the memorandum does not describe the basis for that conclusion. Given that [REDACTED] email account was used to communicate about [REDACTED] allegations, there is probable cause to believe that account may contain additional emails that would elucidate the basis for the Audit Committee's conclusion or provide evidence that the conclusions in the memorandum were pretextual.

28. Similarly, based on my training and experience, I know that iMessages, MMS, and SMS messages oftentimes contain evidence of accounting fraud. For example, as indicated above, messages oftentimes contain evidence relating to shipments to distributors, the timing of those shipments, the need to make revenue numbers or targets, and management pressure or directives regarding those issues. In addition, text messages may contain evidence regarding a user's state of mind, including consciousness of guilt.

29. Additionally, based on my training and experience, I know that browser histories often provide valuable insight into the mindset of individuals who are suspected of securities fraud. In this case, browser history information recovered from the Subject Account would provide valuable

insight into information regarding the users' state of mind, including potential consciousness of guilt and their awareness of the relevant laws and regulations related to revenue recognition and channel stuffing.

30. The requested Warrant and Order will be limited to items sent, received, or created between January 1, 2012 and the present, inclusive, which is the period for which MiMedx has withdrawn (or not issued) financial statements due to a review of "sales and distribution practices."

Evidence, Fruit, and Instrumentalities

31. Based upon the foregoing, I respectfully submit there is probable cause to believe that information stored on the Provider's servers associated with the Subject Account will contain evidence, fruits, and instrumentalities of the Subject Offenses, as more fully described in Section II of Attachment A to the proposed warrant.

32. In particular, I believe the Subject Account is likely to contain the following information:

- Evidence of the user of the Subject Account communicating regarding potential inappropriate revenue recognition practices, such as channel stuffing, and related sales practices at MiMedx, including, but not limited to, communications relating to the timing, quantity, nature and price of any purchase of MiMedx products by distributors/customers and the timing and terms of any payments to MiMedx by the distributors/customers;
- Evidence of the user of the Subject Account communicating regarding earnings and revenue targets or analyst projections;
- Evidence of state of mind, including but not limited to, consciousness of guilt and awareness of any improper revenue recognition practices at MiMedx or awareness of any audits or investigations regarding MiMedx's revenue recognition or sales and distribution practices; and
- Evidence of the geographic location of user of the Subject Account, as well as the computer or device used to access the Subject Account, which may in turn lead to additional evidence.

III. Review of the Information Obtained Pursuant to the Warrants

33. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for service of a search warrant issued under § 2703, or for the collection or production of responsive records. Accordingly, the warrant requested herein will be transmitted to the Provider, which shall be directed to produce a digital copy of any responsive records to law enforcement personnel within 30 days from the date of service. Law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the ESI and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will retain the records and review them for evidence, fruits, and instrumentalities of the Subject Offenses as specified in Section III of Attachment A to the proposed warrant.

34. In conducting this review, law enforcement personnel may use various methods to locate evidence, fruits, and instrumentalities of the Subject Offenses, including but not limited to undertaking a cursory inspection of all emails within the Subject Account. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with emails, including attachments such as scanned documents, pictures, and videos, do not store data as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account, as it is impossible to know in advance all of the unique words or phrases that investigative subjects will use in their communications, and consequently

there are often many communications in an account that are relevant to an investigation but that do not contain any keywords that an agent is likely to search for.

IV. Request for Non-Disclosure and Sealing Order

35. The existence and scope of this ongoing criminal investigation is not publicly known.³

As a result, premature public disclosure of this affidavit or the requested warrant could alert potential criminal targets that they are under investigation, causing them to destroy evidence, flee from prosecution, or otherwise seriously jeopardize the investigation. In particular, given that targets of the investigation are known to use computers and electronic communications in furtherance of their activity, the targets could easily delete, encrypt, or otherwise conceal such digital evidence from law enforcement were they to learn of the Government's investigation.


36. Accordingly, there is reason to believe that, were the Provider to notify the subscriber or others of the existence of the warrant, the investigation would be seriously jeopardized. Pursuant to 18 U.S.C. § 2705(b), I therefore respectfully request that the Court direct the Provider not to notify any person of the existence of the warrant for a period of 180 days from issuance, subject to extension upon application to the Court, if necessary.

37. For similar reasons, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise, except that the Government be permitted without further order of this Court to provide copies of the warrant and affidavit as need be to personnel assisting it in the investigation and prosecution of this matter, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

³ Although newspapers and other media sources have reported that MiMedx is under investigation by regulators, I am aware of no reporting that specifically references [REDACTED] allegation or the fact that members of the company's board of directors may have been complicit in the fraud.

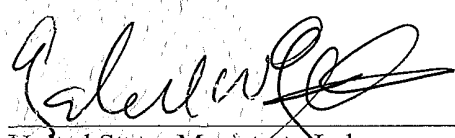
V.Conclusion

38. Based on the foregoing, I respectfully request that the Court issue the warrant sought herein pursuant to the applicable provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) (for contents) and § 2703(c)(1)(A) (for records and other information), and the relevant provisions of Federal Rule of Criminal Procedure 41.



DIANA CHAU
Postal Inspector
United States Postal Inspection Service

Sworn to before me this
31st day of August, 2018



United States Magistrate Judge
Southern District of New York

18 MAG 7548

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant for All Content and
Other Information Associated with the Email
Account [REDACTED], Maintained at
Premises Controlled by Apple, Inc., USAO
Reference No. 2016R00246.

SEARCH WARRANT AND NON-DISCLOSURE ORDER

TO: Apple, Inc. ("Provider")

United States Postal Inspection Service ("Investigative Agency")

1. Warrant. Upon an affidavit of Postal Inspector Diana Chau of the United States Postal Inspection Service, and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds there is probable cause to believe that the email account [REDACTED], maintained at premises controlled by Apple, Inc., contains evidence, fruits, and instrumentalities of crime, all as specified in Attachment A hereto. Accordingly, the Provider is hereby directed to provide to the Investigative Agency, within 30 days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A. The Government is required to serve a copy of this Warrant and Order on the Provider within 14 days of the date of issuance. The Warrant and Order may be served via electronic transmission or any other means through which the Provider is capable of accepting service.

2. Non-Disclosure Order. Pursuant to 18 U.S.C. § 2705(b), the Court finds that there is reason to believe that notification of the existence of this warrant will result in the destruction of or tampering with evidence, or otherwise will seriously jeopardize an ongoing investigation.


Accordingly, it is hereby ordered that the Provider shall not disclose the existence of this Warrant and Order to the listed subscriber or to any other person for a period of 180 days from the date of this Order, subject to extension upon application to the Court if necessary, except that Provider may disclose this Warrant and Order to an attorney for Provider for the purpose of receiving legal advice.

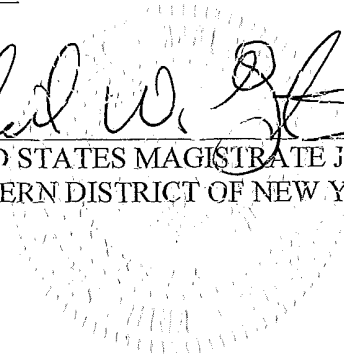
3. Sealing. It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on the Provider; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

August 31, 2018
Date Issued

5:54pm
Time Issued


UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK



Email Search Attachment A

I. Subject Account and Execution of Warrant

This warrant is directed to Apple, Inc. (the "Provider"), headquartered in Cupertino, California, and applies to all content and other information within the Provider's possession, custody, or control associated with the email account [REDACTED].

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below.

II. Information to be Produced by the Provider

To the extent within the Provider's possession, custody, or control, the Provider is directed to produce the following information associated with the Subject Account:

a. *Email content.* All emails sent to or from, stored in draft form in, or otherwise associated with the Subject Account, including all message content, attachments, and header information (specifically including the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email), limited to items sent, received, or created between January 1, 2012 and the date of this Warrant, inclusive;

b. *Images, videos, documents and files.* All pictures, videos, documents, and files posted and/or stored by an individual using the account, including metadata and geotags.

c. *Address book information.* All address book, contact list, or similar information associated with the Subject Account.

d. *Subscriber and payment information.* All subscriber and payment information regarding the Subject Account, including but not limited to name, username, address, telephone number, alternate email addresses, registration IP address, account creation date, account status, length of service, types of services utilized, means and source of payment, and payment history.

e. *Transactional records.* All transactional records associated with the Subject Account, including any IP logs or other records of session times and durations.

f. *Customer correspondence.* All correspondence with the subscriber or others associated with the Subject Account, including complaints, inquiries, or other contacts with support services and records of actions taken.

g. *Web browser history.* All stored information regarding websites accessed by the user of the Subject Account and searches conducted by the user of the Subject Account, limited to content between January 1, 2012 and that date of this Warrant, inclusive;

h. *Service information.* The types of services utilized by the user of the Subject Account.

i. *iOS Backups.* Backups of iOS devices (such as iPhones and iPads) associated with the Subject Account.

j. *Preserved or backup records.* Any preserved or backup copies of any of the foregoing categories of records, whether created in response to a preservation request issued pursuant to 18 U.S.C. § 2703(f) or otherwise.

III. Review of Information by the Government

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the ~~government in this investigation, and outside technical experts under government control~~) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1343 (wire fraud), 1348 (securities fraud), 1350 (improper certification of financial reports by corporate officers); and Title 15, United States Code, Sections 78j(b) and 78ff and Title 17, Code of Federal Regulations, 240.10b-5 (securities fraud), and aiding and abetting and conspiring to commit these offenses in violation of Title 18, United States Code, Section 2 (aiding and abetting), 371 (conspiracy) and 1349 (conspiracy), including the following:

- Evidence of the user of the Subject Account communicating regarding potential inappropriate revenue recognition practices, such as channel stuffing, and related sales practices at MiMedx, including, but not limited to, communications relating to the timing, quantity, nature and price of any purchase of MiMedx products by distributors/customers and the timing and terms of any payments to MiMedx by the distributors/customers;
- Evidence of the user of the Subject Account communicating regarding earnings and revenue targets or analyst projections;
- Evidence of state of mind, including but not limited to, consciousness of guilt and awareness of any improper revenue recognition practices at MiMedx or awareness of any audits or investigations regarding MiMedx's revenue recognition or sales and distribution practices; and
- Evidence of the geographic location of user of the Subject Account, as well as the computer or device used to access the Subject Account, which may in turn lead to additional evidence.